BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Attorney Docket No.: BHT-3111-403

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
Ming-Shiang LAI et al.	:	Group Art Unit: Not Yet Assigned
Application No.: Not Yet Assigned	:	Examiner: Not Yet Assigned
Filed: January 21, 2004	:	

For: **A PROGRAMMABLE DATA PROCESSING APPARATUS FOR CCMP HARDWARE IMPLEMENTATION**

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Taiwanese Application No. 092115620 filed June 10, 2003.**

A certified copy of Applicant's priority document is submitted herewith.

Respectfully submitted,

By: 
Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: January 21, 2004

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder：

申　　請　　日 ： 西元 2003 年 06 月 10 日
Application Date

申　請　案　號 ： 092115620
Application No.

申　　請　　人 ： 揚智科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2003 年 11 月 13 日
Issue Date

發文字號： 09221146940
Serial No.

申請日期：	IPC分類
申請案號： 92115620	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中 文	一種可程式化控制的資料處理裝置
	英 文	
二、發明人（共2人）	姓 名（中文）	1. 賴明祥 2. 張志鵬
	姓 名（英文）	1. 2.
	國 籍（中英文）	1. 中華民國 TW 2. 中華民國 TW
	住居所（中 文）	1. 新竹市東區東南街289號 2. 台北縣板橋市溪生東路279巷12弄16-2號
	住居所（英 文）	1. 2.
三、申請人（共1人）	名稱或姓 名（中文）	1. 揚智科技股份有限公司
	名稱或姓 名（英文）	1.
	國 籍（中英文）	1. 中華民國 TW
	住居所（營業所）（中 文）	1. 台北市內湖路一段246號2樓 （本地址與前向貴局申請者相同）
	住居所（營業所）（英 文）	1.
	代表人（中文）	1. 呂理達
	代表人（英文）	1.

四、中文發明摘要　（發明名稱：一種可程式化控制的資料處理裝置）

一種可程式化控制的資料處理裝置，係利用一儲存單元儲存無線區域網路(wireless LAN, WLAN)加密標準之易變域(mutable fields)，當加密標準變更時，只需修改該儲存單元，以減少硬體其他部分修改，該資料處理裝置包括有：一第一儲存單元，至少儲存一筆輔助資訊，當加密標準變更時，更新該第一儲存單元內所儲存之輔助資訊；一讀取單元，耦接該儲存單元，接收一索引，根據該索引從該第一儲存單元取得該索引所對應之一輔助資訊；以及一處理單元，耦接該讀取單元，接收該輔助資訊及一資料信號，依據該輔助資訊對該資料信號作處理，輸出一處理信號。

五、（一）、本案代表圖為：第 圖三 圖

（二）、本案代表圖之元件代表符號簡單說明：

1- 資料信號　　11- 索引

六、英文發明摘要　（發明名稱：）

四、中文發明摘要　（發明名稱：一種可程式化控制的資料處理裝置）

2-介面裝置
20-第一儲存單元
21-讀取單元
210-輔助資訊
24-第二儲存單元
240-暫存信號
25-協動單元
250-預載入信號
27-處理單元
270-處理信號
271-設定裝置
273-捨棄裝置
274-擷取信號
275-編排裝置
29-第三儲存單元
3-CCM控制邏輯
5-AES加密單元

六、英文發明摘要　（發明名稱：）

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
無			

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

【發明所屬之技術領域】

本發明是關於一種可程式化控制的資料處理裝置，尤指一種應用在無線區域網路(wireless LAN, WLAN)加密標準變更時，可減少硬體修改幅度的可程式化控制的資料處理裝置。

【先前技術】

近年來，隨著無線通信科技的進步，各式各樣的數位行動產品諸如手機、筆記型電腦、PDA實現了人類無線通信的願望，除了擺脫傳統有線電話的束縛，讓使用者更自由，也使人與人間的距離更近。

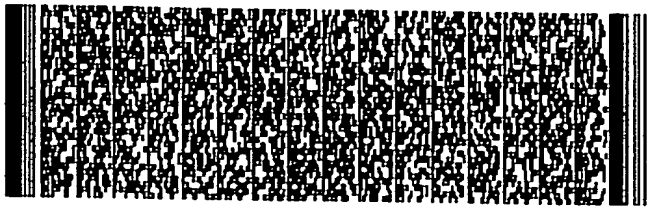
然而，無線網路是利用廣播(broadcast)方式在空間中傳遞。也就是說，只要有心，任何人都可以在空間中擷取到傳輸信號，得知傳輸內容，進而從事偽冒、竄改等危害網路安全的攻擊行為。特別是針對要求傳輸安全的電子商務或是機密文件的應用，更會造成極大的傷害。因此，無線傳輸信號都必需經過加密 (encryption)的動作，以確保傳輸的安全。

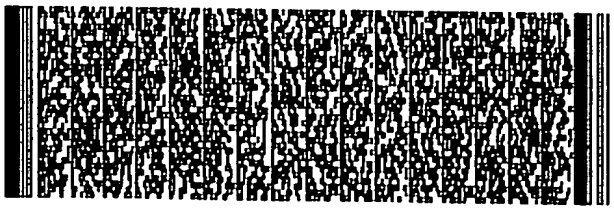
美國電機電子工程學會 (Institute of Electrical and Electronics Engineers, IEEE)，為了加強無線區域網路(wireless LAN, WLAN)的資料傳輸安全，特別制訂了一加密標準：IEEE 802.11i CCMP (Counter-Mode/CBC-MAC Protocol)。CCMP是採用CCM(Counter-Mode with Cipher-Block Chaining Message Authentication Code,

Counter-Mode with CBC-MAC)模式去控制先進加密標準(Advance Encryption Standard, AES)。由於攻擊者所使用方法日新月異，為了確保傳輸資料不易被攻擊成功，無線傳輸安全標準需要不斷的實驗與測試。所以IEEE 802.11i標準仍尚未完全底定。因此，提供CCMP模式下加解密的參數的媒體存取控制服務資料單元(MAC Service Data Unit, MSDU)之訊框標頭(frame header)就有部分欄位被IEEE 802.11i標準定義成易變域(mutable files)。在CCMP的加密過程中，會將易變域欄位捨棄或是設定成0來因應這樣的狀況。

綜上所述，請參閱圖一，此為CCMP的架構圖。CCM控制邏輯3接收傳輸資料，依照標準加密步驟，利用兩個AES加密單元5進行加密的工作，之後再將結果送出。然而隨著標準的改變，資料的格式經常在變更，所以CCM控制邏輯3的硬體設計，特別是接收資料信號1的部分，就必須經常作更新。

由於高科技產業競爭相激烈，時間就是決勝的關鍵。因此，產業不可能等待標準完成才開始進行相關的研發。在同步進行的過程中，會將易變域欄位捨棄或是設定成0，而這些被捨棄或是設定成0的易變域欄位也會拿來作CCM的額外認證資料(Additional Authenticated Data)。只要標準有一點點變更，硬體就必需不斷重新設計以符合需求，除了費時費力，而且沒有效率，因此必需尋求在標準尚未確定下，能夠改善不斷重複設計的硬體架構。





【發明內容】

本發明的主要目的是提供一種可彈性修改的硬體架構，以在標準變更時，減少硬體設計的改變幅度。

為達上述目的，本發明提供一種可程式化控制的資料處理裝置，包括有：

一第一儲存單元，儲存輔助資訊，用以輔助一加密演算法處理資料，其中，當加密演算法變更時，可從外部對應地更新該第一儲存單元所儲存之輔助資訊；

一讀取單元，耦接至該第一儲存單元，接收一索引，以從該第一儲存單元讀取該索引所對應之一輔助資訊；以及

一處理單元，耦接該讀取單元，接收該索引所對應之一資料信號，並依據該索引所對應之輔助資訊，處理該資料信號。

【實施方式】

為使　貴審查委員能對本發明之特徵、目的及功能有更進一步的認知與瞭解，茲配合圖式詳細說明如後：

請參閱圖二，此為本發明之架構圖。本發明的精神在於提供一介面裝置2，利用一儲存體來記錄易變域欄位的變化。當標準變更時，只要更新該記憶體內的資訊，資料信號1一樣藉由該介面裝置2處理後，送入CCM控制邏輯3，達到標準變更欄位目的，而且無須修改CCM控制邏輯3，特

別是輸出入介面部分，因此可以大大地節省硬體設計的時間與功夫。

請參閱圖三，此為本發明之一具體實施例。在此實施例中，本發明包括有：

一第一儲存單元20，至少儲存一筆輔助資訊，當該加密標準變更時，由外部更新該第一儲存單元20內所儲存之輔助資訊。

一讀取單元21，連接該儲存單元20，接收一索引11，根據該索引11從第一儲存單元20取得所對應之一輔助資訊210。取得的方法可以利用查表的方式達成。

一第二儲存單元24，接收一預載入信號250，暫存輸入資料，輸出一暫存信號240；第二儲存單元24主要在暫存所輸入的資料。預載入信號250由該介面裝置的一協動單元25所提供，用來補充訊框標頭(frame header)中所沒有而在加密過程中所必需的資訊，如標頭長度等資訊。

一處理單元27，連接該讀取單元21與該第二儲存單元24，接收輔助資訊210、暫存信號240及資料信號1。處理單元27依據該輔助資訊210對該資料信號1作處理，輸出一處理信號，並將超出一處理長度的資料送到該第二儲存單元暫存。處理單元根據從該輔助資訊對該資料信號的部分位元作捨棄或是設定的工作。因此，該處理單元更包括有：

一設定裝置271，連接該讀取單元21，根據該輔助資訊

210，將該資料信號之部分位元設定成一特定值。該特定值可以設定成為0或是1，端看標準需要而定，一般設定為0。實作上，可利用位元遮罩(bit mask)的形式達成。也就是說，該輔助資訊210在欲設定的位元位址為0，其餘位址為1，在與資料信號1作一個邏輯及(AND)處理，即可得到所求。

一捨棄裝置273，連接該讀取單元21，根據該輔助資訊210，將該資料信號1之部分位元捨棄。加密過程不需要或標準尚未使用的位元就予以捨棄，並將後面位元依次向前遞補，不足的位址補0。

一編排裝置275，該編排裝置有接收經過設定裝置271或捨棄裝置273處理過的擷取信號274的一第一輸入及連接該第二儲存單元的一第二輸入，該編排裝置依該處理長度將該第一輸入及該第二輸入編排後輸出處理信號270，並將超出該處理長度的資料，送到該第二儲存單元24暫存。編排裝置275會優先編排來自該第二儲存單元24的第二輸入。也就是說，編排裝置275會優先將第二儲存單元24所輸入的暫存信號240放在前面，後面在接上第一輸入所接收的擷取信號274。編排裝置的輸出有一個長度限制，超出該處理長度的部分，送到第二儲存單元24，由第二儲存單元24暫存，等待下次的輸出。

本具體實施例中，CCM控制邏輯3輸出與輸入都是128個位元，而資料信號1輸入一次為32個位元。在這種情況

下，還需要一第三儲存單元29，來作介面的處理。該第三儲存單元29，連接該處理單元27，接收該處理信號270，累積到一指定位元數，輸出至一下級電路，也就是CCM控制邏輯3。在本實施例中，該指定位元數就為128，有就是說第三儲存單元29集滿128個位元數才會將資料送到CCM控制邏輯3。

請參閱圖四，繼續利用圖三作一流程說明。資料信號1傳輸一次是32個位元，即4個位元組，表示成D0、D1、D2及D3。在輸入的同時也會有一索引11輸入到讀取單元21，使讀取單元21可至第一儲存單元20取得所對應的輔助資訊210。另外，資料也會輸入協動單元25，由協動單元25將預載入信號250送到第二儲存單元24，第二儲存單元24為3個位元組的暫存器，依序表示成BD0、BD1及BD2。資料首先經過處理單元27，根據讀取單元21所取得之輔助資訊210，設定裝置271將特定位元設定為0，捨棄裝置273將特定位元捨棄，如將D2這位元組捨棄，這時需將D3的值移到D2中，D3中的位元補0。在編排裝置275中，會將第二儲存單元24及經過設定裝置271、捨棄裝置273的擷取信號274載入進來，編排時以第二儲存單元24的暫存信號240優先編排在前，之後再接上擷取信號274，輸出處理長度（本實施例處理長度為4）的處理信號270，超出的部分就送到第二儲存器24暫存，等待下一次輸出。也既是說，BD0、BD1、BD2的資料加上D0共為4個位元組，為處理信號270，而D1與D3就被送到第二儲存單元24暫存，等到下一筆資料

輸入時，D1與D3就會變成BD0與BD1，優先被排在前面輸出。由於CCM控制邏輯3輸出與輸入都是128個位元所以還需要一第三儲存器29將輸出資料暫存，直到累積128位元後再輸出到CCM控制邏輯3，再由CCM控制邏輯3控制加密步驟。

因此，不管標準怎麼變動，所需更改的地方就只侷限在第一儲存單元20內的輔助資訊，而無須變更其他地方的設計。因此在研發期間通常會採用可重複使用的記憶體如可程式化唯讀記憶體(Programmable Read Only Memory, PROM)、可抹除可程式化唯讀記憶體(Erasable Programmable Read Only Memory, EPROM)或是電子式可抹除可程式化唯讀記憶體Electrically Erasable Programmable Read Only Memory, EEPROM)的形式。產品上市時，為降低成本，會採用唯讀記憶體(read only memory, ROM)的形式。可有效解決因標準變動而須大量重複設計的問題。

除了CCMP外，對於另一個的加密標準的選擇：由WiFi聯盟所提出的WPA(WiFi Protected Access)，本發明也可同樣適用。

唯以上所述者，僅為本發明之較佳實施例，當不能以之限制本發明的範圍。即大凡依本發明申請專利範圍所做之均等變化及修飾，仍將不失本發明之要義所在，亦不脫離本發明之精神和範圍，故都應視為本發明的進一步實施狀況。

【圖式簡單說明】

圖一係為CCMP架構圖

圖二係為本發明架構圖

圖三係為本發明之一具體實施例

圖四係為本發明之流程說明

圖號說明：

1-資料信號

11-索引

2-介面裝置

20-第一儲存單元

21-讀取單元

210-輔助資訊

24-第二儲存單元

240-暫存信號

25-協動單元

250-預載入信號

27-處理單元

270-處理信號

271-設定裝置

273-捨棄裝置

274-擷取信號

275-編排裝置

29-第三儲存單元

圖式簡單說明

3-CCM 控 制 邏 輯

5-AES 加 密 單 元

圖式簡單說明

3-CCM 控 制 邏 輯

5-AES 加 密 單 元

六、申請專利範圍

1. 一種可程式化控制的資料處理裝置，包括有：

一第一儲存單元，儲存輔助資訊，用以輔助一加密演算法處理資料，其中，當加密演算法變更時，可從外部對應地更新該第一儲存單元所儲存之輔助資訊；

一讀取單元，耦接至該第一儲存單元，接收一索引，以從該第一儲存單元讀取該索引所對應之輔助資訊；

以及

一處理單元，耦接至該讀取單元，接收該索引所對應之一資料信號，並依據該索引所對應之輔助資訊，處理該資料信號。

2. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該加密演算法為IEEE 802.11i CCMP (Counter-Mode/CBC-MAC Protocol)，該資料信號為無線區域網路(wireless LAN, WLAN)之媒體存取控制服務資料單元(MAC Service Data Unit, MSDU)一部份。

3. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，更包括有一第三儲存單元，耦接至該處理單元，接收經該處理單元處理之資料信號，並待累積到一指定位元數後，輸出至一下級電路。

4. 如申請專利範圍第3項所述之可程式化控制的資料處理裝置，其中該指定位元數為128位元。

5. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該第一儲存單元為一唯讀記憶體(read only memory, ROM)。

六、申請專利範圍

6. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該第一儲存單元為一可程式化唯讀記憶體(Programmable Read Only Memory, PROM)。

7. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該第一儲存單元為一可抹除可程式化唯讀記憶體(Erasable Programmable Read Only Memory, EPROM)。

8. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該第一儲存單元為一電子式可抹除可程式化唯讀記憶體(Electrically Erasable Programmable Read Only Memory, EEPROM)。

9. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該處理單元更包括有一設定裝置，耦接至該讀取單元，根據該索引所對應之輔助資訊，將該資料信號之部分位元設定成一特定值。

10. 如申請專利範圍第9項所述之可程式化控制的資料處理裝置，其中該特定值為0與1之其中之一。

11. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該處理單元更包括有一捨棄裝置，耦接至該讀取單元，根據該索引所對應之輔助資訊，將該資料信號之部分位元捨棄。

12. 如申請專利範圍第1項所述之可程式化控制的資料處理裝置，其中該處理單元更包括一編排裝置，該編排裝置有輸入資料的一第一輸入及接收一第二儲存單元之

六、申請專利範圍

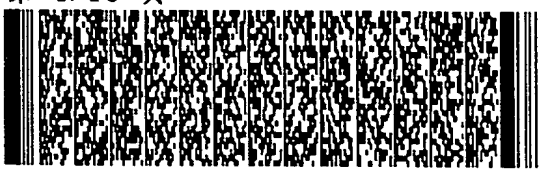
一暫存信號的一第二輸入，該編排裝置依一處理長度將該第一輸入及該第二輸入編排後輸出，並將超出該處理長度的資料，送到該第二儲存單元暫存。

13. 如申請專利範圍第12項所述之可程式化控制的資料處理裝置，其中該第二儲存單元，耦接至該處理單元之該編排裝置，該第二儲存單元接收一預載入信號及由該處理單元所輸入之超出該處理長度的資料，暫存輸入資料，輸出該暫存信號至該處理單元之該編排裝置。

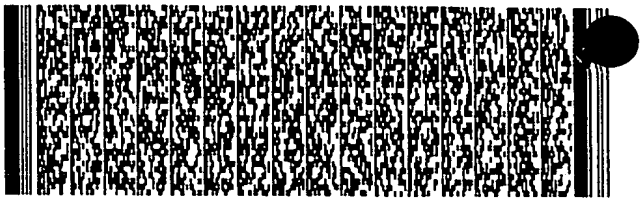
14. 如申請專利範圍第13項所述之可程式化控制的資料處理裝置，其中該編排裝置會優先編排來自該第二儲存單元的第二輸入。

15. 如申請專利範圍第13項所述之可程式化控制的資料處理裝置，其中該第二儲存單元為一暫存器(register)。

第 1/16 頁



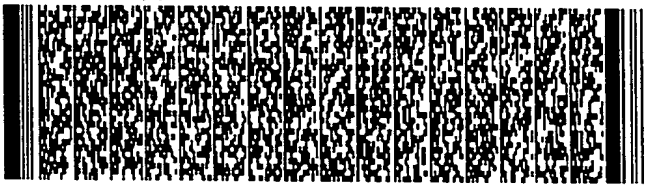
第 2/16 頁



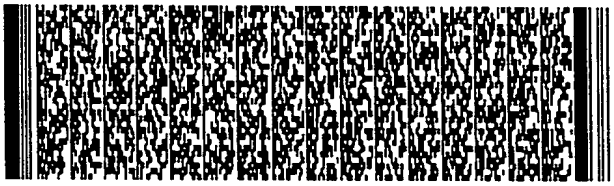
第 3/16 頁

第 4/16 頁

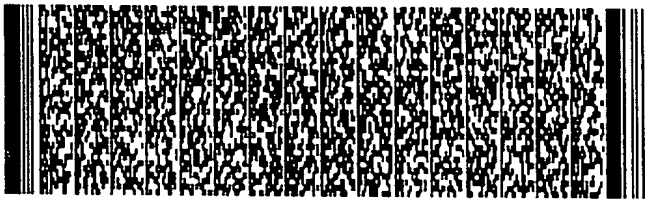
第 5/16 頁



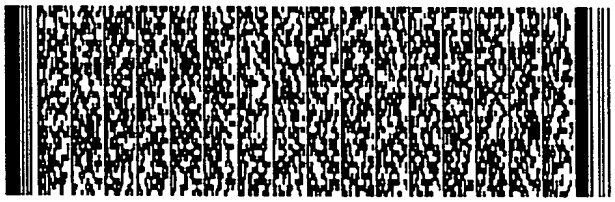
第 5/16 頁



第 6/16 頁



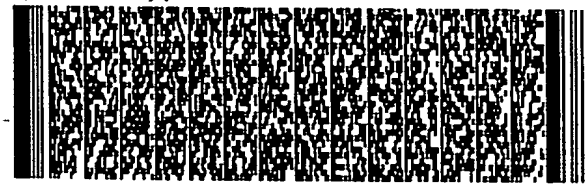
第 6/16 頁



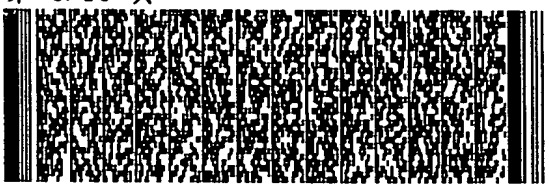
第 7/16 頁

第 7/16 頁

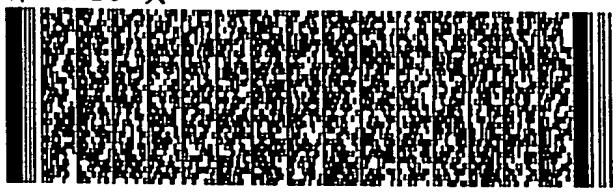
第 8/16 頁



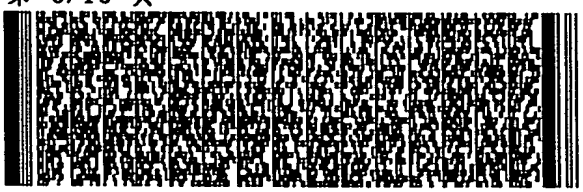
第 8/16 頁



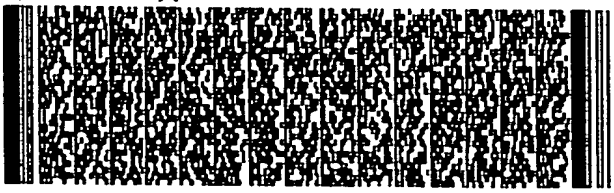
第 9/16 頁



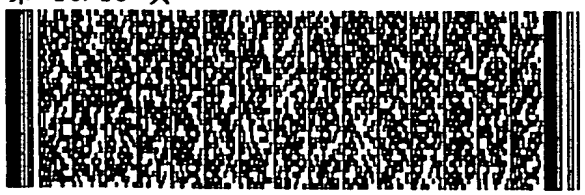
第 9/16 頁



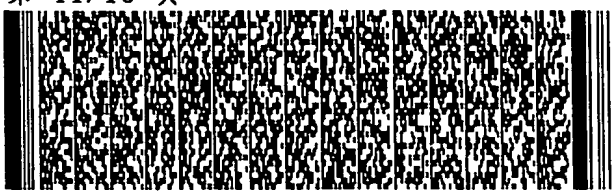
第 10/16 頁



第 10/16 頁

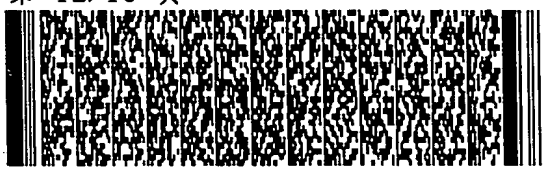


第 11/16 頁



第 11/16 頁

第 12/16 頁

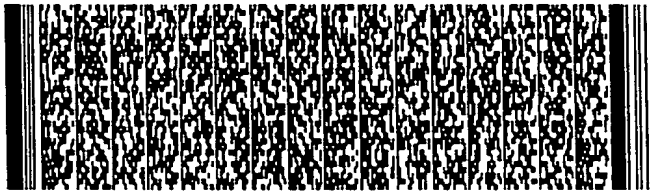


第 13/16 頁

第 14/16 頁

第 14/16 頁

第 15/16 頁



第 16/16 頁

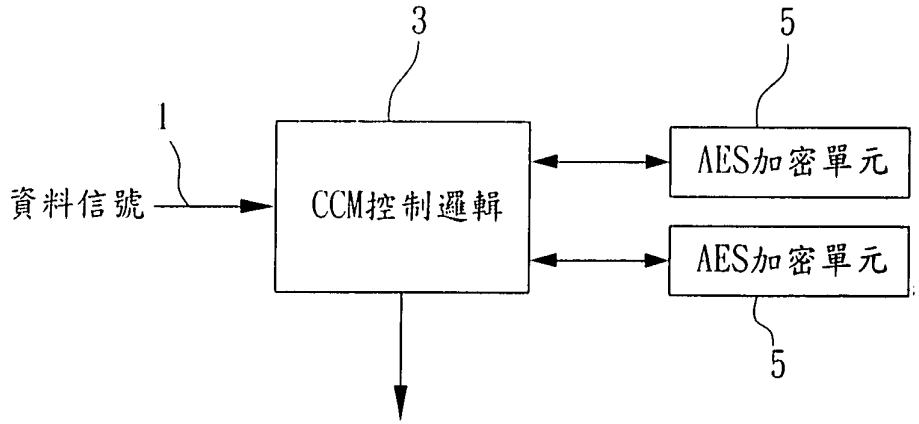

3
5
1
資料信號
CCM控制邏輯
AES加密單元
AES加密單元
5

圖 一

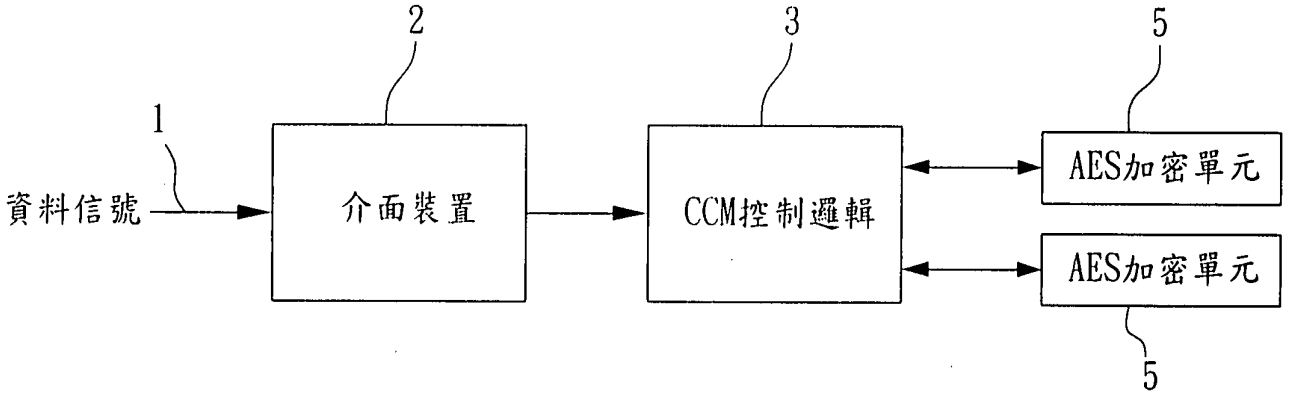

2
3
5
1
資料信號
介面裝置
CCM控制邏輯
AES加密單元
AES加密單元
5

圖 二

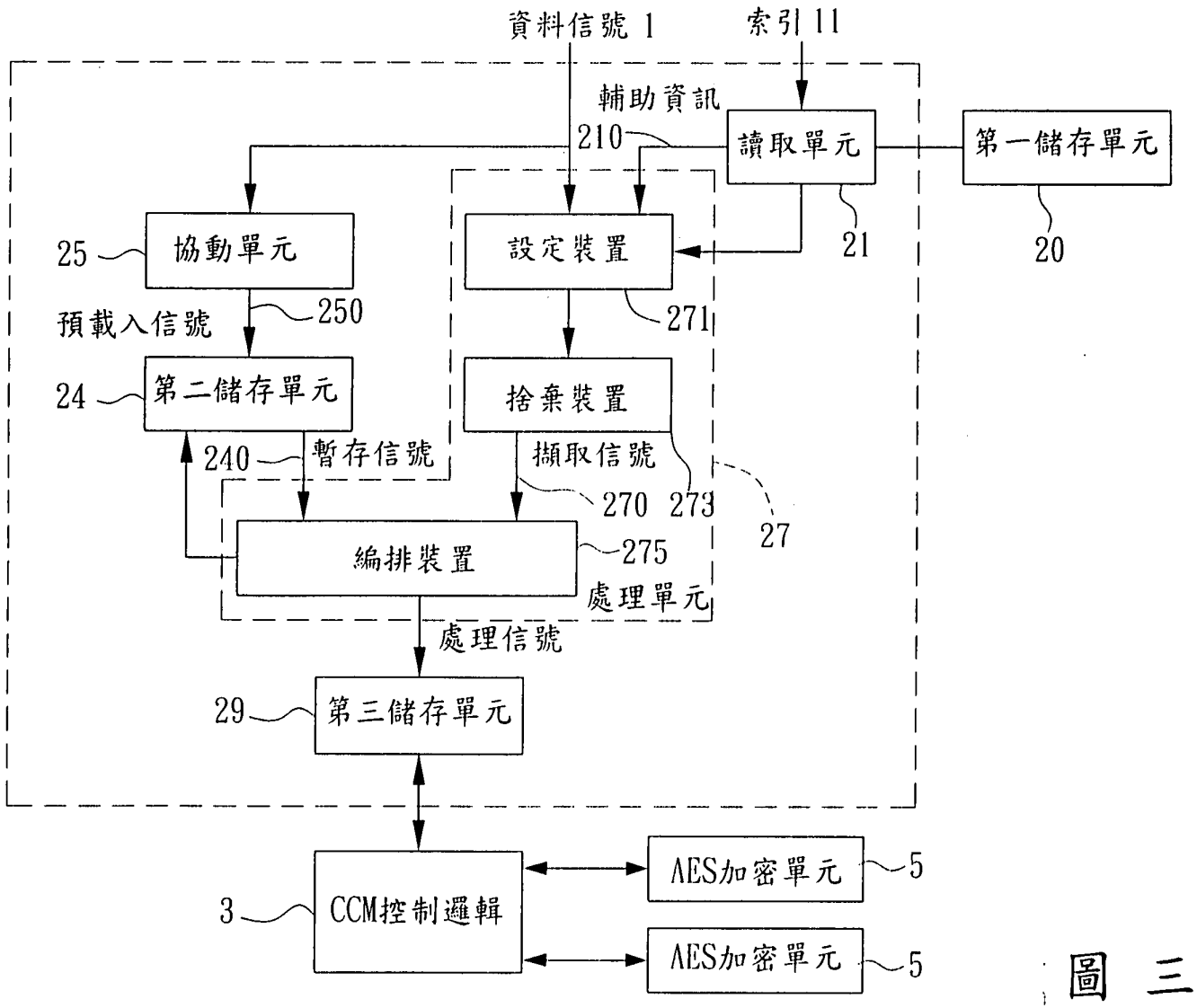

資料信號 1
索引 11
輔助資訊
210
讀取單元
第一儲存單元
20
21
25
協動單元
設定裝置
271
預載入信號
250
24
第二儲存單元
捨棄裝置
240
暫存信號
擷取信號
270
273
27
編排裝置
275
處理單元
處理信號
29
第三儲存單元
3
CCM控制邏輯
AES加密單元
5
AES加密單元
5

圖 三

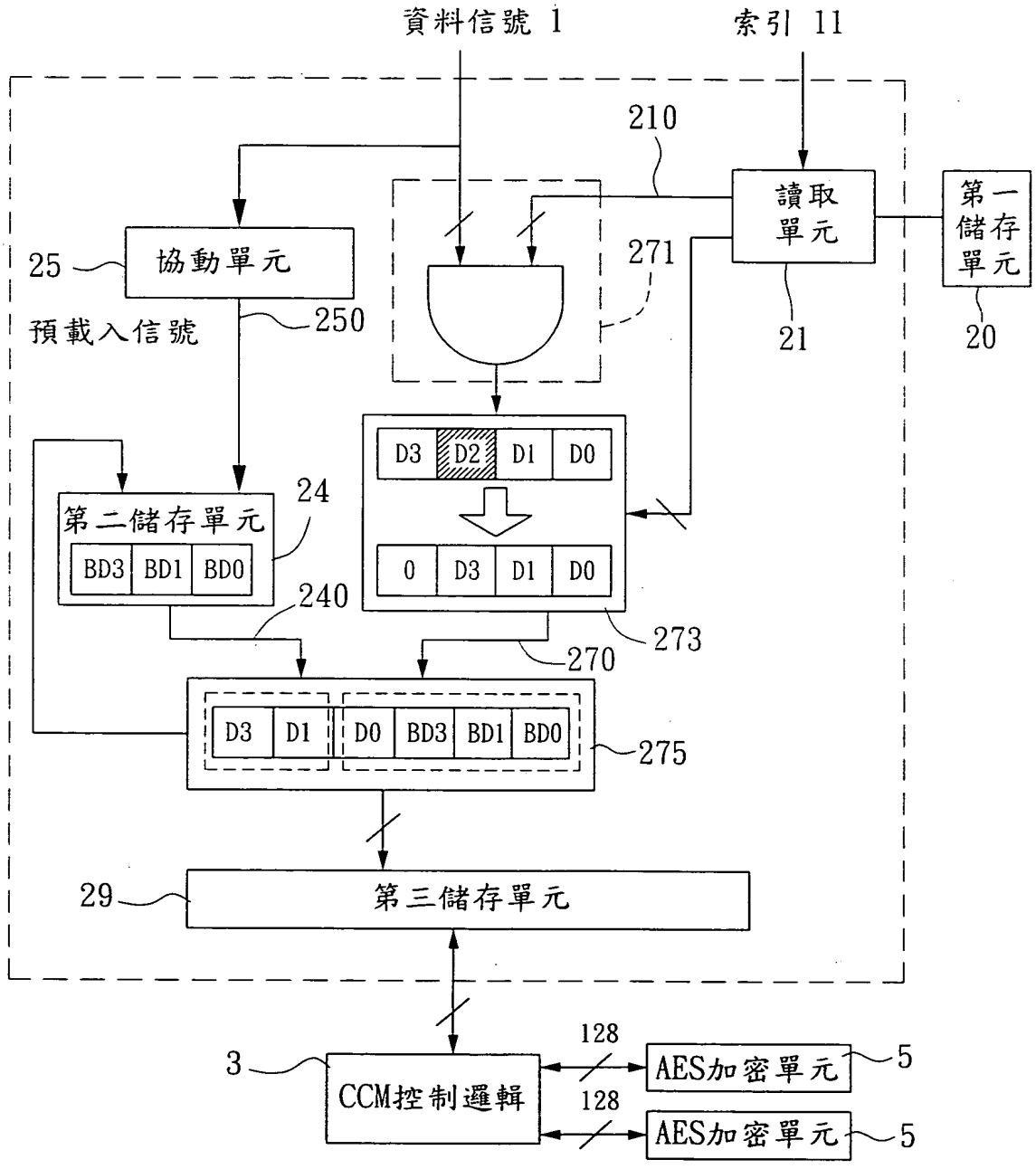

資料信號 1
索引 11
210
讀取單元
第一儲存單元
20
21
271
25
協動單元
預載入信號
250
D3 D2 D1 D0
0 D3 D1 D0
273
24
第二儲存單元
BD3 BD1 BD0
240
270
D3 D1 D0 BD3 BD1 BD0
275
29
第三儲存單元
3
CCM控制邏輯
128
AES加密單元
5
128
AES加密單元
5

圖 四